UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,223	08/16/2001	Thomer Michael Gil	12221-007001	2855

26161 7590 06/06/2006

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
NAWAZ, ASAD M	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 06/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,223	GIL ET AL.	
	Examiner	Art Unit	
	Asad M. Nawaz	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21 and 50-77* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21 and 50-77* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the Appeal Brief filed 3/10/06. Claims 1-21 and 50-77 were previously presented. No claims have been added, amended, or canceled. Accordingly, claims 1-21 and 50-77 are pending.

Response to Arguments

2. Applicant's arguments, see Appeal Brief, filed 3/10/06, with respect to the rejection(s) of claim(s) 1-21 and 50-77 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Lyle et al (USPN: 6,971,028) further in view of Hsu et al (USPN: 6,098,157).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 63 stands rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. More specifically it is not clear what is further comprising.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 63-68 and 70-75 rejected under 35 U.S.C. 102(e) as being anticipated by Lyle et al (USPN: 6,971,028) hereinafter referred to as Lyle.

As to claim 63, Lyle teaches a method of monitoring traffic flow in a monitor device disposed to receive network traffic packets comprises:

Producing statistics corresponding to a parameter of traffic flow to trace the source of an attack (Fig 9, 908-310; col 2, lines 45-50; col 7, lines 3-12; sniffers are used in analyzing and evaluating traffic flows to scrutinize suspicious activity in an attempt to ascertain the source of an attack), with producing further comprising:

Mapping the traffic flow into a plurality of buckets (col 7, lines 43-67; event data, which is defined as suspicious data is placed in a queue as a set corresponding to a single incident)

Varying the number of buckets according to the amount of traffic and number of flows according to down traffic flow into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in the bucket (col 7, line 43 to col 8, line 5; col 13, lines 42-50; once an event (a set of data corresponding to an attack) is placed in the queue, other event data is grouped or combined with existing event data to associate related events into a single incident object. Also, events that do not bear similarities on their face may also be combined or aggregated based upon

event rate in a given network or sub-network. Thus varying the amount of event data sets destined for the analysis framework module).

As to claim 64, Lyle teaches the method of claim 63 wherein varying varies the number of buckets so that the monitoring device is not vulnerable to DoS attacks against its own resources (col 19, lines 37-45; the protocol disclosed by Lyle teaches a strong protection against denial of service attacks as well as other forms of attacks).

As to claim 65, Lyle teaches the method of claim 63 wherein varying the number of buckets comprises: comparing the number of buckets to a threshold number of buckets, determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold and as the number of buckets changes, the buckets have values derived from the buckets prior to the change (col 7, lines 43 to col 8, line 33; a statistics database is consulted including a threshold based upon incident rate to determine in part whether or not the event data set should be combined or split. Once a decision is made, variables within the event data set essentially remain the same).

As to claim 66, Lyle teaches the method of claim 63 wherein further comprising comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance (col 7, lines 32-42 and col 8, lines 6-14; many thresholds, such as incident rate, preconfigured criteria, timestamps, etc, are considered in determining the significance or importance of a possible attack)

As to claim 67, Lyle teaches the method of claim 63, wherein comparing statistic values comprises accumulating statistic values from the packets and comparing the

values accumulated in the buckets to thresholds that depend on the number of buckets. (col 7, lines 3-20 and 43-67; sniffers are utilized in capturing packet content as well as data related to packets. Thereafter, the data requiring further analysis and/or evaluation is discerned and stored and placed into a queue for further scrutiny by the tracking system).

As to claim 68, Lyle teaches the method of claim 63 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored so that the monitoring device is not vulnerable to a denial of service attack against its own resources (col 19, lines 37-45; the protocol disclosed by Lyle teaches a strong protection against denial of service attacks as well as other forms of attacks).

Claim 70 is essentially the computer product residing on a computer readable medium of claim 63 and thus rejected under similar rationale.

Claim 71 is essentially the computer product residing on a computer readable medium of claim 64 and thus rejected under similar rationale.

Claim 72 is essentially the computer product residing on a computer readable medium of claim 65 and thus rejected under similar rationale.

Claim 73 is essentially the computer product residing on a computer readable medium of claim 66 and thus rejected under similar rationale.

Claim 74 is essentially the computer product residing on a computer readable medium of claim 67 and thus rejected under similar rationale.

Claim 75 is essentially the computer product residing on a computer readable medium of claim 68 and thus rejected under similar rationale.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-21, 50-62, 69, and 76-77 rejected under 35 U.S.C. 103(a) as being unpatentable over Lyle further in view of Hsu et al (USPN: 6,098,157) hereinafter referred to as Hsu.

As to claim 1, Lyle teaches a method of monitoring traffic flow in a monitor device disposed to receive network traffic packets comprises:

Producing statistics corresponding to a parameter of traffic flow to trace the source of an attack (Fig 9, 908-310; col 2, lines 45-50; col 7, lines 3-12; sniffers are used in analyzing and evaluating traffic flows to scrutinize suspicious activity in an attempt to ascertain the source of an attack), with producing further comprising:

Mapping the traffic flow into a plurality of buckets (col 7, lines 43-67; event data, which is defined as suspicious data is placed in a queue as a set corresponding to a single incident)

Accumulating statistics from the packets and comparing the number of buckets to a threshold (col 7, lines 32-42 and col 8, lines 6-14; many thresholds, such as incident rate, preconfigured criteria, timestamps, etc, are considered in determining the significance or importance of a possible attack)

Determining whether to vary the number of buckets according to the amount of traffic and number of flows according to down traffic flow into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in the bucket (col 7, line 43 to col 8, line 5; col 13, lines 42-50; once an event (a set of data corresponding to an attack) is placed in the queue, other event data is grouped or combined with existing event data to associate related events into a single incident object. Also, events that do not bear similarities on their face may also be combined or aggregated based upon event rate in a given network or sub-network. Thus varying the amount of event data sets destined for the analysis framework module).

Although Lyle does teach the use of hash functions in a unique way to efficiently communicate with the system (see col 19, lines 11-36), however, Lyle does not explicitly indicate the use of a hash function to output an integer corresponding to one of the buckets.

Hsu teaches a using a hash to output an integer corresponding to the location of a location of a unique bucket identifier (see fig 8, col 4, lines 26-38; col 5, lines 18-23)

It would have been obvious to one with ordinary skill in the art at the time the invention was made to combine the disclosure of Lyle with the hashing techniques in Hsu to make the system more efficient. Using the hashing technique, which utilizes addresses, will output the unique bucket identifier quickly. Because Lyle also uses addresses to relate event data to aggregate events into a single incident object, the use of Hsu's hashing technique would work seamlessly.

As to claim 2, Lyle teaches the method of claim 1 wherein the buckets are storage areas in a memory space (abstract, col 7, lines 46-50; event sets are stored in queues that are also part of the overall memory space of the resident computing device).

As to claim 3, Lyle teaches the method of claim 1 wherein as the number of buckets changes, the buckets have values derived from the buckets prior to change (col 7, liens 59-67 events related to a single incident are combined to produce a single object that has data corresponding with the event database).

As to claim 4, Lyle and Hsu teach the method claim of claim 1 wherein the hash function adapts to map to the new number of buckets, as the new number of buckets changes (col 4, lines 26-38; the bucket identifier is unique and if a bucket is eliminated, so is its corresponding identifier. If, on the other hand, a bucket is added, a unique identifier is created).

As to claim 5, Lyle teaches the method of claim 1, wherein comparing statistic values comprises accumulating statistic values from the packets and comparing the values accumulated in the buckets to thresholds that depend on the number of buckets. (col 7, lines 3-20 and 43-67; sniffers are utilized in capturing packet content as well as data related to packets. Thereafter, the data requiring further analysis and/or evaluation is discerned and stored and placed into a queue for further scrutiny by the tracking system).

As to claim 6, Lyle teaches the method of claim 1 wherein the parameter is the count of how many packets a data collector or gateway examines (col 7, lines 3-20 and

43-67; sniffers are utilized in capturing packet content as well as data related to packets including the number of packets collected).

As to claim 7, Lyle teaches the method of claim 1 wherein as a value of a parameter approaches a threshold, the monitoring device raises an alarm (see fig 9, col 8, lines 15-53; a policy database is consulted in determining what action should be taken, such a sending alarms)

As to claim 8, Lyle teaches the method of claim 1 wherein the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets (Figs 11 A and B)

As to claim 9, Lyle teaches the method of claim 1 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored so that the monitoring device is not vulnerable to a denial of service attack against its own resources (col 19, lines 37-45; the protocol disclosed by Lyle teaches a strong protection against denial of service attacks as well as other forms of attacks).

As to claim 10, Lyle teaches the variable number of buckets efficiently identifies the source or sources of attack by breaking down traffic into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in each bucket (col 8, lines 34-53; the event along with the policy assigned for that event is used in tracking the attack back to its origin, the incident object to which the event was designated would in fact identify the source of the attack).

As to claim 11, Lyle teaches the method of claim 1 wherein the traffic is monitored at multiple levels of granularity, from aggregate to individual flows (col 7, lines

3 to col 8, line 53; individual packets to events to incident objects are analyzed and evaluated at numerous times during processing of given information)

As to claim 12, Lyle teaches the method of claim 1 wherein the method of claim 1 is applied to monitoring of TCP packet rations and repressor traffic (col 7 line 59 to col 8, line 4; traffic from numerous types of networks including tcp/ip based networks is used and numerous values included in the statistics database are disclosed).

As to claim 13, Lyle teaches the method of claim 1 wherein further comprising comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance (col 7, lines 32-42 and col 8, lines 6-14; many thresholds, such as incident rate, preconfigured criteria, timestamps, etc, are considered in determining the significance or importance of a possible attack)

Claims 14-21, 50-62 and 76-77 are essentially the computer program product and data collector for the above-mentioned method claims and are thus rejected under similar rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Asad M. Nawaz whose telephone number is (571) 272-3988. The examiner can normally be reached on M-F 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AMN

Philip Tran
PRIMARY EXAMINER